Configurer l'authentification unique SAML avec Google

Publié: 2023-09-19

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités de Google.

Avant de commencer

- Vous devez être familiarisé avec l'administration de Google Admin.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures nécessitent de copier et de coller des informations entre le système ExtraHop et la console Google Admin, il est donc utile d'avoir les deux systèmes ouverts côte à côte.

Activer SAML sur le système ExtraHop

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Authentification à distance**.
3. Dans la liste déroulante Méthode d'authentification à distance, sélectionnez **SAML**.
4. Cliquez sur **Continuer**.
5. Cliquez sur **View SP Metadata (Afficher les métadonnées SP)**.
6. Copiez l'URL ACS et l'ID de l'entité dans un fichier texte. Vous collerez ces informations dans la configuration Google lors d'une procédure ultérieure.

Ajouter des attributs personnalisés à l'utilisateur

1. Connectez-vous à la console d'administration de Google.
2. Cliquez sur **Utilisateurs**.
3. Cliquez sur l'icône Gérer les attributs personnalisés  .
4. Cliquez sur **Ajouter un attribut personnalisé**.
5. Dans le champ Catégorie, tapez `ExtraHop`.
6. Optionnel : Saisissez une description dans le champ Description.
7. Dans la section Champs personnalisés, entrez les informations suivantes.
   a) Dans le champ Nom, tapez `writelevel`.
   b) Dans la liste déroulante Info Type, sélectionnez **Text**.
   c) Dans la liste déroulante Visibilité, sélectionnez **Visible pour le domaine**.
   d) Dans la liste déroulante Nombre de valeurs, sélectionnez **Valeur unique**.
8. Activer l'accès au module NDR
   a) Dans le champ Nom, tapez `ndrlevel`.
   b) Dans la liste déroulante Type d'information, sélectionnez **Texte**.
   c) Dans la liste déroulante Visibilité, sélectionnez **Visible pour le domaine**.
   d) Dans la liste déroulante No. of values, sélectionnez **Single Value**.
9. Activer l'accès au module NPM
   a) Dans le champ Nom, tapez `npmlevel`.
   b) Dans la liste déroulante Info Type, sélectionnez **Text**.
   c) Dans la liste déroulante Visibilité, sélectionnez **Visible pour le domaine**.

d) Dans la liste déroulante Nombre de valeurs, sélectionnez **Valeur unique**.

10. Optionnel : Si vous avez connecté des magasins de paquets, activez l'accès aux paquets en configurant un champ personnalisé avec les informations suivantes.
    a) Dans le champ Nom, tapez `packetslevel`.
    b) Dans la liste déroulante Type d'information, sélectionnez **Texte**.
    c) Dans la liste déroulante Visibilité, sélectionnez **Visible pour le domaine**.
    d) Dans la liste déroulante Nombre de valeurs, sélectionnez **Valeur unique**.
11. Cliquez sur **Ajouter**.

Ajouter les informations du fournisseur d'identité de Google au système ExtraHop

1. Dans la console d'administration Google, cliquez sur l'icône du menu principal et sélectionnez **Applications** > **Applications SAML**.
2. Cliquez sur l'icône Activer le SSO pour une application SAML.
3. Cliquez sur **SETUP MY OWN CUSTOM APP**.
4. Sur l'écran Google IdP Information, cliquez sur le bouton **Download** pour télécharger le certificat(`GoogleIDPCertificate.pem`).
5. Retournez aux paramètres d'administration du système ExtraHop.
6. Cliquez sur **Ajouter un fournisseur d'identité**.
7. Saisissez un nom unique dans le champ Nom du fournisseur. Ce nom apparaît sur la page de connexion du système ExtraHop.
8. Dans l'écran Google IdP Information, copiez l'URL SSO et collez-la dans le champ SSO URL de l'appareil ExtraHop.
9. Dans l'écran Google IdP Information, copiez l'Entity ID et collez-le dans le champ Entity ID du système ExtraHop.
10. Ouvrez le `certificat GoogleIDPC` dans un éditeur de texte, copiez-en le contenu et collez-le dans le champ Certificat public du système ExtraHop.
11. Choisissez l'une des options suivantes pour provisionner les utilisateurs.
    - Sélectionnez **Auto-provision users** pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lorsque l'utilisateur se connecte pour la première fois.
    - Décochez la case **Approvisionnement automatique des utilisateurs** et configurez manuellement de nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Les niveaux d'accès et de privilèges sont déterminés par la configuration de l'utilisateur dans Google.
12. L'option **Activer ce fournisseur d'identité** est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter, décochez la case.
13. Configurez les attributs des privilèges des utilisateurs. Vous devez configurer l'ensemble des attributs utilisateur suivants avant que les utilisateurs puissent se connecter au système ExtraHop par l'intermédiaire d'un fournisseur d'identité. Les valeurs sont définies par l'utilisateur, mais elles doivent correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne sont pas sensibles à la casse et peuvent inclure des espaces. Pour plus d'informations sur les niveaux de privilèges, voir Utilisateurs et groupes d'utilisateurs.

    Important: Vous devez spécifier le nom de l'attribut et configurer au moins une valeur d'attribut autre que **Pas d'accès** pour permettre aux utilisateurs de se connecter.

    Dans l'exemple ci-dessous, le champ Nom de l'attrib ut est l'attribut de l'application et la Valeur de l'attribut est le nom du champ utilisateur configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`urn:extrahop:saml:2.0:writelevel`
Administration du système et des accès	`illimité`
Privilèges d'écriture complets	`full_write`
Privilèges d'écriture limités	`limited_write`
Privilèges d'écriture personnels	`personal_write`
Privilèges de lecture seule complète	`lecture_complète`
Privilèges restreints en lecture seule	`lecture_restreinte`
Pas d'accès	`aucun`

14. Configure l'accès au module NDR.

Champ	Exemple Valeur de l'attribut
Nom de l'attribut	`urn:extrahop:saml:2.0:ndrlevel`
Accès complet	`complet`
Pas d'accès	`aucun`

15. Configure l'accès au module NPM.

Champ	Exemple Valeur de l'attribut
Nom de l'attribut	`urn:extrahop:saml:2.0:npmlevel`
Accès complet	`complet`
Aucun accès	`aucun`

16. Optionnel : Configurer les paquets et l'accès aux clés de session. La configuration des paquets et des attributs de clé de session est facultative et n'est requise que lorsque vous disposez d'un packetstore connecté.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	`urn:extrahop:saml:2.0:packetslevel`
Paquets et clés de session	`full_with_keys`
Paquets uniquement	`complet`
Paquets tranches seulement	`tranches`
Pas d'accès	`aucun`

17. Cliquez sur **Save**.
18. Sauvegarder la configuration en cours d'exécution.

Ajouter les informations du fournisseur de services ExtraHop à Google

1. Retournez à la console d'administration Google et cliquez sur **Suivant** sur la page Informations Google Idp pour passer à l'étape 3 de 5.

2. Saisissez un nom unique dans le champ Nom de l'application pour identifier le système ExtraHop. Chaque système ExtraHop pour lequel vous créez une application SAML doit avoir un nom unique.
3. Optionnel : Saisissez une description pour cette application ou téléchargez un logo personnalisé.
4. Cliquez sur **Suivant**.
5. Copiez l'URL de l'Assertion Consumer Service (ACS) du système ExtraHop et collez-la dans le champ ACS URL de Google Admin.

   Note: Vous devrez peut-être modifier manuellement l'URL ACS si elle contient un nom d'hôte inaccessible, tel que le nom d'hôte par défaut du système `extrahop`. Nous vous recommandons de spécifier le nom de domaine complet du système ExtraHop dans l'URL.
6. Copiez l'ID de l'entité SP du système ExtraHop et collez-le dans le champ ID de l'entité dans Google Admin.
7. Cochez la case **Réponse signée**.
8. Dans la section Name ID, ne modifiez pas les paramètres par défaut **Basic Information** et **Primary Email**.
9. Dans la liste déroulante Format de l'ID de nom, sélectionnez **PERSISTANT**.
10. Cliquez sur **Suivant**.
11. Sur l'écran Attribute Mapping, cliquez sur **ADD NEW MAPPING**.
12. Ajoutez les attributs suivants exactement comme indiqué. Les quatre premiers attributs sont obligatoires. L'attribut `packetslevel` est facultatif et n'est requis que si vous avez un packetstore

connecté. Si vous avez un packetstore et que vous ne configurez pas l'attribut `packetslevel`, les utilisateurs ne pourront pas afficher ou télécharger les captures de paquets dans le système ExtraHop.

Attribut d'application	Catégorie	Champ utilisateur
`urn:oid:0.9.2342.19200300.100.1.3`	Informations de base	Courriel principal
`urn:oid:2.5.4.4`	Informations de base	Nom de famille
`urn:oid:2.5.4.42`	Informations de base	Prénom
`urn:extrahop:saml:2.0:writelevel`	ExtraHop	niveau d'écriture
`urn:extrahop:saml:2.0:ndrlevel`	ExtraHop	ndrlevel
`urn:extrahop:saml:2.0:npmlevel`	ExtraHop	npmlevel
`urn:extrahop:saml:2.0:packetslevel`	ExtraHop	packetslevel

13. Cliquez sur **Finish (Terminer**), puis sur **OK**.
14. Cliquez sur **Edit Service**.
15. Sélectionnez **Activé pour tout le monde**, puis cliquez sur **Enregistrer**.

Attribuer des privilèges aux utilisateurs

1. Cliquez sur **Utilisateurs** pour revenir au tableau de tous les utilisateurs de vos unités organisationnelles.
2. Cliquez sur le nom de l'utilisateur que vous souhaitez autoriser à se connecter au système ExtraHop.
3. Dans la section Informations sur l'utilisateur, cliquez sur **Détails de l'utilisateur**.
4. Dans la section ExtraHop, cliquez sur **Niveau d'écriture** et saisissez l'un des niveaux de privilèges suivants.

   - `illimité`
   - `écriture_complète`
   - `écriture_limitée`
   - `écriture_personnelle`
   - `lecture_complète`
   - `lecture_limitée`
   - `aucun`

   Pour plus d'informations sur les privilèges des utilisateurs, voir Utilisateurs et groupes d'utilisateurs.
5. Optionnel : Si vous avez ajouté l'attribut `packetslevel` ci-dessus, cliquez sur **packetslevel** et saisissez l'un des privilèges suivants.

   - `complet`
   - `complet_avec_écriture`
   - `aucun`

6. Optionnel : Si vous avez ajouté l'attribut `detectionslevel` ci-dessus, cliquez sur **detectionslevel** et tapez l'un des privilèges suivants.
   - `complet`
   - `aucun`
7. Cliquez sur **Enregistrer**.

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur **Se connecter avec** *<nom du fournisseur>*.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse électronique et de votre mot de passe. Vous êtes automatiquement dirigé vers la page de présentation d'ExtraHop.